Dynamic DES Encryption

Akash Mukherjee and Ankush Sharma,
akash.mukherjee.ece12@iitbhu.ac.in *ankush.sharma.ece12@iitbhu.ac.in*
Indian Institute of Technology (B.H.U.), Varanasi, India

Summary

Due to rise of quantum computers which leads to faster computation, there is an increasing interest in the field of physical layer security. This paper presents an idea involving some physical layer technique to drastically change the intactness of symmetric key encryption protocols, viz. DES, AES. Our invention combines physical layer security with cryptographic protocols to some extent, resulting into stronger cipher. Current work shows how we can achieve greater security in symmetric key encryption protocols. This paper gives a new way to look at wireless security. With the given analysis and the plots we can surely predict how much promising the field of Physical Layer Security is. Besides, if we use it properly, we can even stand strong against the rise of faster computation. The solution provided for the limitations of symmetric key encryption can easily implemented practically, since, due to the purpose of quality improvement of service, service providers already use the channel characteristics detection mechanism at the transmitter node.

Key words:

Physical Layer Security, DES, Key management, Cryptanalysis, Quantum Cryptanalysis, Round Keys.

1. Introduction

Symmetric key encryption protocols give an upper limit on the number of messages to be sent using a fixed key without compromising with the security. So, for a busy network it becomes an absolute necessary to replace the old key with a newer one time to time to avoid unwanted persons from interfering in the communication. Another serious issue with the conventional Data Encryption Standards a.k.a. DES produces exactly same cipher for a fixed message, that makes it a little helpful for an eavesdropper to eavesdrop upon. To address these kind of limitation, a promising field of physical layer security is emerging out in the cyber security scenario. In Physical Layer Security, depending upon the wireless channel between the communicators, we vary the encryption mechanism. This channel dependent encryption on one hand makes the protocol dynamic or time dependent, and on the other hand helps increasing the robustness against several attacks. Especially with the rise of quantum computers, capable of computing faster than traditional ones, time dependent encryption becomes an absolute necessary. This paper presents a quantitative analysis of such limitation as well as provides a possible solution. In 1949, when Shannon talked about perfect secrecy in his paper Communication Theory of Secrecy Systems [3], he stated that to achieve a perfect secrecy the key length should at-least be equal to the message length. But due to practical reasons we can not make key as long as message, it would be waste of a large memory. Since, may be perfect secrecy is not what we wish for, we just want our personal thing to stay personal. So, we have a trade-off for key length, which we are ready to compromise with. DES uses a 56 bit key with 8 bits for error correction. From this remaining 48 bit key, 16 round sub-keys are generated. For stronger cipher we want this sub-keys to be unrelated ideally. Since, they are generated from the main key, by some means they are related, this compromises with the security of DES. Our version of modified DES uses channel property to select key for each stage. Here we need to establish a connection between transmitter and receiver before we start communication. So, even if the adversary is present on the same channel, he will not be able to extract the key because synchronization would be required at the first place. Here, synchronization means there would be a kind of handshake, before communication starts through exchanging known pilot signal. Current protocol also addresses the active attack where the attacker may not only wants to intercept the message but also be interested in tempering the data. One of such attacks is Man in the middle attack. Rest of the paper will be organized as follows: in Section II. we will be talking the core idea we are presenting followed by some results we have got through simulations in Section III., and finally in Section IV. we will conclude the paper

DOI : 05.IJIS.2016.1.2

with some future prospects and some disadvantages of the idea presented here.

2. Tables, Figures and Equations

Our current work addresses two main issues of the existing DES. First one is the same cipher output for fixed plain text which sometimes proven advantageous for the attacker, and the other one is randomness in the round-keys generated from a fixed main key. In this section we will analyze each of them one by one, and will propose our solution for those.

2.1 Fixed Cipher Output: To figure out the key, sometimes attackers use the knowledge of similar cipher getting produced from same plain text. For instance, in formal message some letter head or some part of the message remains unchanged, that in turn results into some known message-cipher pair which gives the adversary a fair advantage. To avoid this we are proposing a method where we alter some bits in the cipher based on through what channel the message is passing. One of the assumption here is at the transmitter we have the channel knowledge, which can be realized easily [4]. Every wireless channel can be treated as some discrete system [5], where the input signal is the transmitted one (x[m]) and the output signal is the received signal (y[m]), considering some additive noise (w[m]) in the channel, we can model it as, $y[m] = h[m]x[m] + w[m]$ where, h is the channel fading, we will use it as channel characteristics in the rest of this paper. During link establishment between legitimate communicators, a known pilot career will be sent through the channel, from which the channel characteristics will be deduced with a negligible error, that too can be reduced using some modern techniques like Forward Error Correcting Codes (FEC) or Automatic Repeat Request (ARQ) [4]. The plot between the error probability and Signal to Noise ratio (SNR)

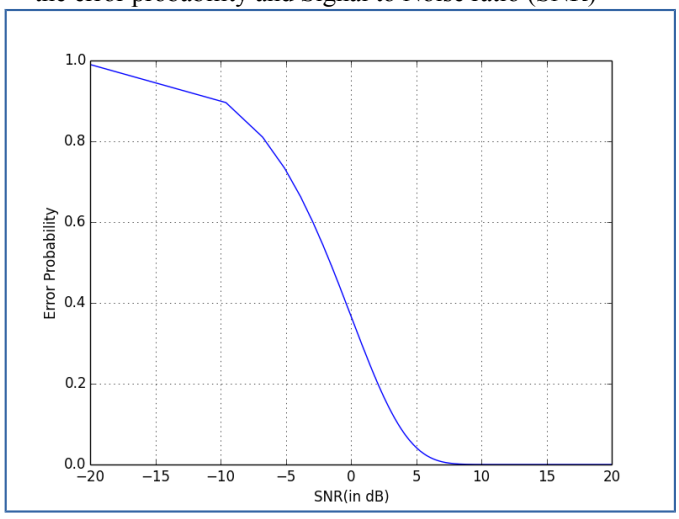

Fig. 1 Error in channel detection

From the plot we can see error is reduced to 0 around SNR 7.5 dB. Which further can be reduced by deploying modern methods mentioned above.

Once we get the channel characteristics (h) correctly, to make the DES encryption dynamic we flip particular number of bits of the final cipher output of each encrypted block. Since, DES is a block cipher with block size 64 bit; to ensure at-least one bit flip we can use h %64 (modulo operator) to select particular bits to be flipped. One possible implementation would be by mapping channel fading characteristics to a 64 bit binary number and XOR this with the final cipher. Apart from this to add some extra level of security in our form of DES, we have used channel dependent assignment of each characters. In other words, instead of converting the message into a bit stream through ASCII coding, we rather liked random channel dependent dictionary. In that case, even with the key handed to the attacker, he additionally need to figure out the assignment. For instance, if we map each character to an 8 bit binary number, there would be 256C97 possible cases of assignment, which is nearly 3 E+72.

2.2 Random Keys: Sometimes strength of a symmetric key encryption depends upon how strong the key is. A strong key is the one when altered even for one bit, can produce a different cipher altogether. In practice, messages are not typically 64 bit, so they gets encrypted block-by-block. But the same key gets used each time. This opens up a broader scope of cryptanalysis. Having knowledge about some message-cipher pair, and key expansion/ round key generation mechanism attacker might be able to get his hands on the actual data in whole or in part. Our physical layer based solution to this problem is just to select separate keys for different blocks. We propose to have a key table for each contacts and depending upon the wireless media in-between a particular key is selected at both the sides. This might lead to some extra storage but, once a key got selected its size is same as before, so memory wastage will not be there during operation, with this used in CBC mode (Cipher Block Chaining) we can achieve a zenith of security.

2.3 Man in the middle attack: Generally, to avoid such active attacks we use hash or checksum part with the cipher for network layer implementations. Here we designed similar protocol to provide data integrity through exploitation of channel properties. Unlike putting fixed block at the beginning of the cipher, we have added a fixed size block at a variable position. So, a normal question, how it's going to help with integrity? As, we have added the extra block from a variable position in-between, the interpreter would not have any idea about its location, so if he wants to change the message, there is a possibility of changing that block.

DOI : 05.IJIS.2016.1.2

3. Results

Analysis of the proposed methodology will require some ground works to be done. To essay the strength of a cipher, first we need to define the constraints for the adversary, what are the resources they have. We assume the adversary has a set of known message-cipher pair. Additionally he can be at any position, the worst case for security is he present near the recipient, although he would require some sort of synchronization. With this information in hand adversary is trying to predict cipher for a message. Let us start the quantitative analysis. In the below figure challenger is the legitimate sender and there is an adversary, unaware about the channel mechanism of the encryption. So, what the adversary does is having q number of known message-cipher pair, he is trying to predict given a new cipher whether m0 or m1 got encrypted.

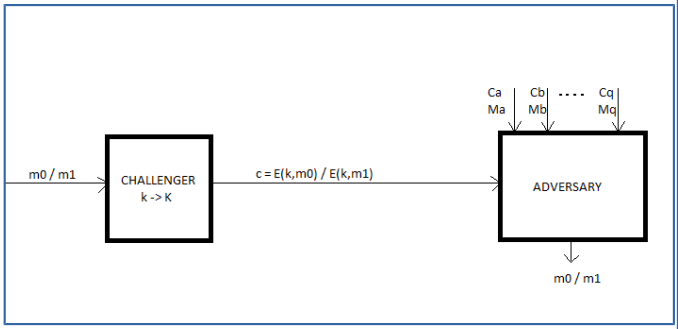

Fig. 2 Adversary Model

We define,

$$Adv[E,K] = Pr[m0 \text{ is encrypted}] - Pr[m1 \text{ is encrypted}]$$

Here, 'Adv' is the adversary power, it is defined as the ability of the attacker to predict which one of the message is encrypted by the challenger. In other words, this is the measure of the probability with which the adversary is correct about predicting the cipher. For a semantically secure cipher we want it to be negligible. Throughout this paper we have typically taken this value to be $1/2^{32}$. With q queries of message length L, and key set size |X|, term $q^2L^2/|X|$ has the major contribution in Adv[E,K] and we want it to be less than $1/2^{32}$,

$$q^2L^2/|X| < 1/2^{32}, \quad (1)$$

in DES the key size is 56 bits, so the size of the key space is 2^{56}. That would limit qL up to 2^{12}, which gives us an upper limit of 32 KB data to be encrypted before we should change the key. That is a quite low value. With our proposal, as instead of using one single key, we are using a key table, out of which we select one; let us assume we have n number of keys in that table. So, to successfully decrypt a message attacker need to know all of them, because the encryption is dynamic as explained in the previous section.

Hence, we can assume the key table into a virtual key of length 56n. So, we can do the similar proceedings as above. To test its robustness, we need to consider one thing before getting started, as the key using for encryption is not same all the time, the adversary need to interpret more messages to get same number of message-cipher pair. We can replace 'q' by 'q/n' in (1).

$(q/n)^2L^2/|X| < 1/2^{32}$, now the key space size has became 2^{56n}. So, we have got the plot between the number of entries in the key table versus message size before we need to change the key.

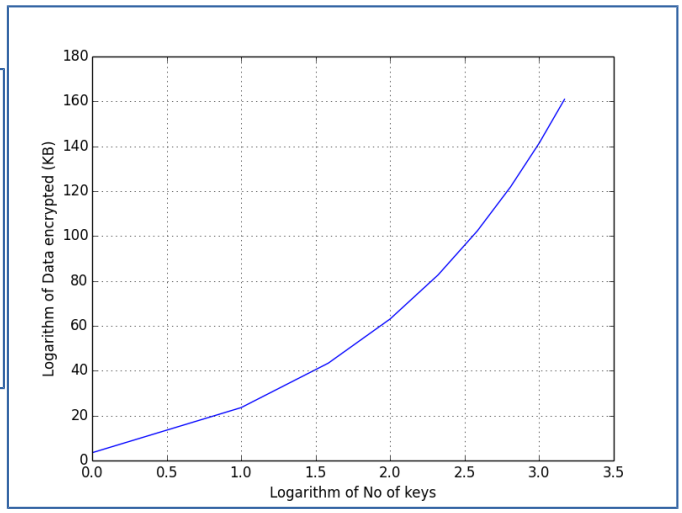

Fig. 3 Key replacement policy

Above plot depicts, with the increasing number of keys, the size of the data getting encrypted before key replacement keeps on increasing. But, there is a trade off; but we can see that with 8 keys in the table, we will be able encrypt 10^{140} KB data before the key to be changed.

This was for the key management. Now, if we look towards the time to break a cipher with brute-force, it is known [6] that for normal computers this can be done in linear number of computation with Key, i.e. O(|K|). But, as talked earlier about the quantum computers this can even be decreased down to $O(|K|^{1/2})$ [7]. For, existing DES this comes to some milliseconds for a GHz processor. With our modification on, Fig. 4 is the plot between the time to break a cipher versus the number of key entries in the key table.

DOI : 05.IJIS.2016.1.2

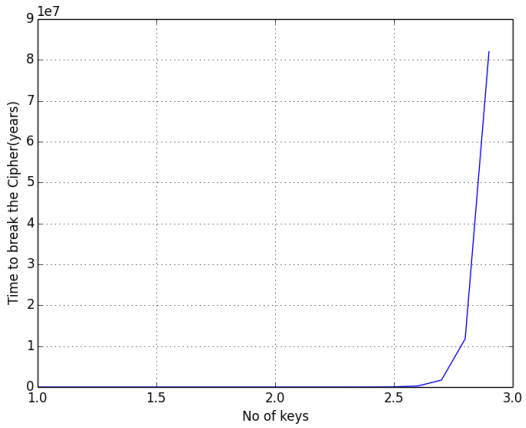

Fig. 4 Strength of Key

Clearly from the above plot, we can see how drastically the strength of the cipher increases with small increase in the entries. Even with only three entries in the table, we are getting above 90 million years span. For a hypothetical terahertz computer will only be able to break the cipher in 90000 years.

Acknowledgments

We would like to extend our gratitude towards our parents and friends who always motivated us for doing something new, something original. We would like to thank Mr. Nikhil Gupta for his help during editing earlier version of the manuscript. We would also like to thank Dr. K. V. Srinivas for sharing some invaluable thoughts. Without their efforts it would not be possible to convert our idea into a presentable format.

References

[1] "Data encryption standards, network security standards", Vol 394, pp 49-67, 1997, Springer US.

[2] J. Daemen and V. Rijmen. "The design of rijndael aes – the advanced encryption standards". Springer-Verlag, 2001.

[3] C. E. Shannon. "A mathematical theory of communications". Bell System Technical Journal. July 1948. pp 623.

[4] S. Sain. Thesis No. 1154. "Modeling and characterization of wireless channels in harsh environment". Malrdalen University School of Innovation, Design and Engineering.

[5] D. Tse and P. Vishwanathan. "Fundamentals of wireless communications". Cambridge University Press. 2005.

[6] D. Coppersmith, "The data encryption standards and its strength against attacks", IBM Journal of Research and Development, Vol 38, Issue 3, pp 243-250, 1994.

[7] Grover, Lov K. "Quantum computer can search arbitrarily large databases by a single query". Phys. Rev. Letters (1997). pp 4709-4712.

[8] E. Biham and A. Shamir, "Differential cryptanalysis of data encryption standards", Springer-Verlag, 1993

[9] "Quantum safe cryptography and security an introduction, benefits, enablers and challenges". June 2015 ISBN No. 979-10-92620-03-0 ETSI White Paper No. 8

[10] R. Willson, D. Tse, and R. Scholtz. "Channel identification: secret sharing and reciprocity in ultrawideband channels". IEEE Transactions on Information Forensics and Security. 2(3):364 375. 2007

Akash Mukherjee currently pursuing the B.Tech in Indian Institute of Technology (B.H.U.), Varanasi, will be graduated in 2016. He had worked for Indian Defence R & D Laboratory.

Ankush Sharma currently pursuing B.Tech on Indian Institute of Technology (B.H.U.), Varanasi, will be graduated in 2016. He has experience in working with Google.

DOI : 05.IJIS.2016.1.2